UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,322	03/02/2004	Dmitry Andreev	END920030143	1826

7590 07/31/2007

Andrew M. Calderon
Greenblum and Bernstein P.L.C.
1950 Roland Clarke Place
Reston, VA 20191

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
07/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

5

Office Action Summary	**Application No.** 10/791,322	**Applicant(s)** ANDREEV ET AL.	
	Examiner Amare F. Tabor	**Art Unit** 2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *03/02/2004*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-22 are examined.

Specification

2. The abstract of the disclosure is objected to because the abstract contains more than 150 words. Correction is required. See MPEP § 608.01(b).

3. In the abstract, the term "LDAP" should be spelled out as "lightweight directory access protocol."

4. Claim 22 is objected to because of the following informalities: claim is numbered as "Claim 22:" - should be numbered as "22". Appropriate correction is required.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 9-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 9 and 15, including the respective dependent claims 10-14 and 16-20, recite computer program that are not tangibly embodied on an appropriate computer-readable storage medium; thus the claims do not constitute statutory subject matter.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5-6, 8, 15, 19-20 and 22 are rejected under 35 U.S.C. 102(b) as being anticipated by Wenisch, et al (US Pub No.: 2003/0033545 A1, cited by applicant and now US Pat No.: 7,100,054 B2), referred as "***Wenisch***" hereinafter.

7. *<u>As per claim 1</u>*, Wenisch discloses,

A method for authentication in a network, the method comprising: (Par. [0004], lines 1-3, "in one embodiment of the invention, a method is provided for authenticating a user of a computer over a computer network").

- creating a credential string which is derived from a session ID; (Par. [0004], lines 9-11, "the challenge string can be either a sequence number or a session identifier or another numerical or alphanumerical identifier"). The "challenge string" is "credential string" as claimed.

- sending a UserID associated with the session ID and the credential string to a software application; (see FIG. 2 and Par. [0020], lines 1-4, "the security applet 18 is provided with a challenge string, such as a unique session identification (ID) or a sequence number, and an encryption key as parameters from a web server"). Wenisch further discloses, (Par. [0021], lines 1-5, "the login packet 20 can, but not necessarily, contain the challenge string, and the password or other credentials in encrypted form and a hash of the data in these three fields").

- receiving a confirmation request which includes the credential string; (Par. [0005], lines 6-8, "receive a login packet having the challenge string and a password that is encrypted using the first encryption key").

- and sending a response in reply to the confirmation request to validate the credential string to authenticate the UserID; (Par. [0005], lines 1-3 and 8-10, "in another embodiment of the invention, a system is provided for authenticating a user of a computer over a computer network") and ("and authenticate the password by using information provided by an authentication provider").

8. *As per claim 2*, Wenisch discloses,

- the step of maintaining a password at a portal and not sending the password to authenticate the UserID ; (see FIG. 2 and Par. [0020], lines 4-8, "when the user transmits the login form to the web server by clicking a login button or some other means, the security applet 18 in the hidden frame retrieves the user name and password from the login form, and creates a login packet to be sent to the web server").

9. *As per claim 3*, Wenisch discloses,

- wherein the credential string is an encrypted hash of the session ID (abstract, lines 11-15, "the login packet can further include a user name, wherein the session identification, the user name, and the password are encrypted. Additionally, the login packet can include a hash of the session identification, the user name, and the password").

10. <u>*As per claim 5*</u>, Wenisch discloses,

- wherein the sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in persistent memory (Par. [0021], lines 9-5, "after the login packet is transmitted to the web server 14, the security applet 18 resides in the hidden frame of the computer 12 the username, session ID, and password of the user until the user closes their browser or accesses a different web page other than one associated with the secure page supplied from the web server 14").

11. <u>*As per claim 6*</u>, Wenisch discloses,

- sending the UserID associated with the session ID and the credential string to a software application proxy; (see FIG. 2 and Par. [0023], lines 4-8, "the web server 14 then transmits to the authentication provider 16 authentication data including the username and encrypted credentials and requests that the authentication provider verify the authentication data").

- checking whether the session ID and credential string has been previously received within a predetermined time period; (Par. [0026], lines 9-12, "to provide additional security, the session ID preferably expires if the user doesn't make a page request after a predetermined time interval").

- and if affirmative, initiating a security breach procedure (Par. [0027], lines 1-5, "FIG. 3 shows an illustrative example of how he web server 14 of FIG. 1 can also authenticate each form response submitted to the web server to prevent against falsified or modified form data from being submitted to the web server").

12. <u>*As per claim 8*</u>, Wenisch discloses,

- wherein the receiving step and sending a response step is performed by an authentication proxy (Par. [0024], lines 1 to Par. [025], line 3, "the authentication provider 16 receives and decrypts the authentication data and validates it using a security method, such as NT.RTM system call. The authentication provider 16 then creates a response for the web server 14 by hashing the decrypted credentials and a secret string").

13. <u>*As per claim 15*</u>, Wenisch discloses,

A system for authenticating a session, comprising: an authentication proxy which receives requests to authenticate a UserID and credential string; (Par. [0030], lines 1-3, "a method of authenticating a form submitted by the user of a computer network of FIG. 1 will now be described with reference to FIG. 5").

- and a credential string validation component which receives requests to validate the credential string; (Par. [0030], lines 13-14, ("at 66, the fields and the values entered on the form are authenticated").

- wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period (rejection of claim 6 is applied to similar limitation).

14. *As per claim 19,*

This claim recites similar limitation similar to that of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

15. *As per claim 20*, Wenisch discloses,

- a portal to create and encrypt the credential string by hashing a session ID, the portal sends the credential string and the UserID to the software application proxy, and does not send a password associated with the UserID (Par. [0028], lines 1-10, "a program, using code such as JavaScript, can be used to transmit data from the form to the web server when the user fills out and submits the form to the web server. The program can collect the name and contents of each field in the form and the session number provided for this form request and pass this data to the hidden security applet which still is in memory in the hidden frame. The security applet then creates authentication data 30 including a hash code of the session ID, sequence number, plaintext user password, and all fields and values on the web form").

16. *As per claim 22*, rejection of claim 1 is incorporated and Wenisch further discloses,

A computer program product comprising a computer usable medium having readable program code embodied in the medium (Par. [0006], lines 1-5, "in yet another embodiment of the invention, an article of manufacture is provided that includes a computer readable medium having computer readable program code for authenticating a user of a client computer over a computer network").

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 7, 9-14, 16-18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wenisch (US Pub No.: 2003/0033545 A1) as applied to the claims above, and further in view of Shrader et al. (US Pat No.: 6,374,359 B1), referred as "***Shrader***" hereinafter.

18. <u>As per claim 4</u>, Wenisch does not explicitly disclose,

- performing a lightweight directory access protocol (LDAP) lookup using the UserID;

- and if the LDAP lookup confirms the UserID and the response validates the credential string, returning a successful authentication reply to the software application for establishing a session associated with the session ID, otherwise sending an unsuccessful authentication reply to the software application

However, in the same filed of endeavor, Shrader discloses the above limitation as, (see FIG. 2 and column 2, lines 65-67, "the given server application, in one embodiment, is a Lightweight Directory Access Protocol (LDAP) GUI interface"); and

(See FIG. 3 and column 5, lines 50-60, "at step 56, the LDAP GUI Web server CGIs check to see if the user name and password are valid. This is accomplished, for example, by calling the appropriate LDAP API to determine whether the user seeking to log in exists in the directory. If the outcome of the test at step 56 indicates that the user name and password are not valid, the GGIs issue a user name and password error message at step 58 and control returns to step 52. If, however, the outcome of the test at step 56 indicates that the username and password are valid, the routine continues at step 60 ").

Therefore, it would have been obvious to one of having ordinary skill in the art, at the time the invention was made, to combine the teachings of Shrader into the method of Wenisch, because one of ordinary skill in the art would want to secure access to a LDAP authentication interface running on a Web server (see Shrader FIG. 3).

19. <u>*As per claim 7*</u>, claim 6 is incorporated and Wenisch further discloses,

- wherein the security breach procedure causes the termination of any session associated with the UserID (Par. [0025], lines 1-3 and 9-10, "the authentication provider 16 then creates a response for the web server 14 by hashing the decrypted credentials and a secret string") and ("if the hash code 26 is correct, then the web server 14 grants the user access to the web site"). Thus, implying that termination would occur if the hash code 26 were incorrect.

20. <u>*As per claim 9 and 10*</u>, Wenisch discloses,

Method for authenticating a user request for a software application, the method comprising: receiving a UserID and credential string at an authentication proxy server; (Par. [0007], lines 2-5, the authentication provider can be an authentication server or can be a software program installed on the computer in communication with the computer network").

- sending a confirmation request from the authentication proxy to a portal, the confirmation request includes the credential string; and receiving a response at the authentication proxy for the confirmation request; (see rejection of claim 1 above, as applied to this limitation).

- and validating the UserID (Par. [0030], lines 13-14, ("at 66, the fields and the values entered on the form are authenticated").

Wenisch does not explicitly disclose,

- using a light weight directory access protocol (LDAP) lookup request and the response

However, Shrader discloses the above limitation as, (column 4, lines 10-18, "as is well-known, the Web server accepts a client request and returns a response. The communication between the browser and the server is conducted using HTTP protocol. According to the present invention, it is assumed that the Web server supports a server application to which the user (at the client) desires access. By way of example only, the server application is an administration interface, such as the Lightweight Directory Access Protocol (LDAP) GUI CGI interface").

Therefore, it would have been obvious to one of having ordinary skill in the art, at the time the invention was made, to combine the teachings of Shrader into the method of Wenisch, because one of ordinary skill in the art would want to validate user's request to access a Web server (see Shrader column 4, lines 27-34).

21. *<u>As per claim 11 and 14</u>*, Wenisch discloses,

- receiving the UserID and a password during a logon to the portal, wherein the UserID is validated in the validating step and the password is maintained at the portal and used to process the confirmation request; and creating the credential string from a session ID at the portal (Par. [0020], line 4 to Par. [0021], line 3, " when the user transmits the login form to the web server by clicking a login button or some other means, the security applet 18 in the hidden frame retrieves the user name and password from the login form, and creates a login packet to be sent to the web server. The login packet 20 can, but not necessarily, contain the challenge string, such as the session ID provided by the server").

22. *<u>As per claim 12</u>*, Wenisch discloses,

- encrypting the credential string (Par. [0004], lines 3-7, "the method includes transmitting an applet having a designation, such as a challenge string, and a first encryption key, receiving a login packet having the challenge string and a password that is encrypted using the first encryption key").

23. *<u>As per claim 13</u>*, Wenisch does not explicitly disclose,

- validating the confirmation request by assuring the credential has been received only once for confirmation at the portal, otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy (Par. [0013], "it is still another object of this invention to ensure that a first user logs off from a web server completely so that a subsequent user cannot use the first user's userid and password to access protected documents or services").

24. *<u>As per claim 16 and 17,</u>*

These claims recite similar limitations to that of claim 4, thus rejected with the same rationale applied against claim 4 above.

25. *<u>As per claim 18</u>*, Wenisch discloses,

- wherein the authentication proxy receives the UserID and credential string from a software application (rejection of claim 1 above is applied to this limitation).

26. *As per claim 21*, Wenisch discloses,

- a portal for accepting a logon by a user and for creating the credential string from an associated session ID; (rejection of claim 20 above is applied to this limitation).

Wenisch does not explicitly disclose,

- a lightweight directory access protocol (LDAP) directory for authenticating UserIDs and which is accessible by the authentication proxy;

However, Shrader discloses the above limitation as, (column 4, lines 27-32, "before using the functionality provided by the LDAP GUI from their Web browsers, users or administrators need to enter their LDAP user name (or distinguished name) and password on a login panel. These values are sent to the Web server and validated by the LDAP GUI CGIs").

- and a software application proxy for intercepting the UserID and credential string sent by the portal for monitoring duplicate occurrences of the UserID and credential string (see rejection of claim 13, as applied to this limitation)

Therefore, it would have been obvious to one of having ordinary skill in the art, at the time the invention was made, to combine the teachings of Shrader into the method of Wenisch, because one of ordinary skill in the art would want the LDAP interface authenticate the user for administrative or directory tasks (see Shrader column 4, lines 45-51).

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892)

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare F. Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on (571) 270-1392. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AFT

Chameli C Das
CHAMELI DAS
SUPERVISORY PATENT EXAMINER
7/30/07